UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	S2 11 Cr. 878 (LAK)
- v. -	:	
TIMUR GERASSIMENKO,	:	
Defendant.	:	

GOVERNMENT'S SENTENCING SUBMISSION

PREET BHARARA
United States Attorney for the
Southern District of New York,
Attorney for the United States of America.

SARAH Y. LAI
Assistant United States Attorney
—Of Counsel—

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

July 20, 2015

Honorable Lewis A. Kaplan
United States District Judge
Southern District of New York
500 Pearl Street, Room 2240
New York, New York 10007

Re: *United States* v. *Timur Gerassimenko*, S2 11 Cr. 878 (LAK)

Dear Judge Kaplan:

Sentencing in the above-referenced matter is scheduled for July 23, 2015, at 3:00 p.m. The Government respectfully submits this memorandum in advance of sentencing to provide the Court with additional information regarding the relative roles of the defendants and the impact of the offenses of conviction. Details regarding the fraudulent scheme are in the Indictment and the Presentence Investigation Report ("PSR"), and will not be repeated here. For the reasons discussed below, the Government respectfully requests that a sentence within the parties' Stipulated Guidelines Range of 78 to 97 months be imposed.

I. The Defendants and Their Roles

The defendants, all Estonian nationals, were members of a cybercriminal enterprise that operated for years with the assistance of coconspirators in Russia and the Ukraine. Each has pleaded guilty to conspiracies to commit wire fraud and to distribute malicious software known as the DNS Changer Malware. This Malware altered the domain name system ("DNS") settings of infected computers so that the defendants were able to direct those computers, without the computer owners' consent, to websites and advertisements that generated millions of dollars for members of the conspiracy. The defendants also intentionally blocked infected computers' ability to access antivirus software and operating system security updates, which would otherwise have detected and neutralized the Malware.

As discussed below, defendant Vladimir Tsastsin was the leader of the conspirators in Estonia. Defendant Timur Gerassimenko employed the programmers who participated in the conspiracy, including defendant Valeri Aleksejev. Defendant Dmitri Jegorov was the lead network administrator and employed the network administrators for the conspiracy, including defendant Anton Ivanov. Defendant Konstantin Poltev was the public face of the enterprise and actively concealed the true nature of the conspiracy from, among other entities, banks, search engine companies, web hosting providers, and advertisers. In terms of their relative roles, the evidence shows that Tsastsin was the primary decision-maker; Gerassimenko was Tsastsin's

closest associate and right-hand man; Jegorov, Poltev and Aleksejev implemented Tsastsin's plans; and Ivanov was at the lowest level.

A. Vladimir Tsastsin

Tsastsin was the founder and leader of a company called Rove Digital since approximately early 2002. Since at least 2007, Tsastsin began using Rove Digital to commit online advertising fraud. Tsastsin had connections to coconspirators in Russia who provided him with the DNS Changer Malware. He also had Russian connections, including Andrey Taame, who had experience in selling fraudulent Internet traffic to online advertising networks. In approximately 2009, following negative publicity resulting from his conviction of Estonian felony charges (further discussed below), Tsastsin ceased using Rove Digital but continued its advertising fraud scheme by breaking up its functions among a number of different companies, nominally headed by certain of his co-defendants. For example, an entity named Infradata, which listed co-defendant Timur Gerassimenko as its sole board member, took over the computer programming side of the fraud scheme. Another company, named Novatech, which listed co-defendant Dmitri Jegorov as its sole board member, maintained the critical online infrastructure which supported the fraud scheme. Tsastsin used still other companies – including the SPB Group, Cernel, Internet Path and others – to register domain names and IP addresses and to rent computer infrastructure, including rogue DNS servers, that were used as instrumentalities of the fraud scheme. Tsastsin himself was the director of a purported computer consulting firm named IT Consulting, but, in fact, was the head of the overall operation. (The various companies controlled by Tsastsin will be referred to, collectively, as the "Rove Companies.") In addition, Tsastsin also operated a Danish entity named Furox APS, while his Russian partner and co-defendant Andrei Taame (who remains a fugitive), operated companies named Lintor Ltd and Onwa Ltd, through which they sold hijacked (redirected) clicks to online advertisers. Payment records from advertising networks and bank records showed that U.S.-based advertisers alone paid millions to members of the conspiracy for the fraudulent web traffic. The bulk of the money went into bank accounts controlled by Tsastsin, his wife, his parents, Taame, and Gerassimenko.

In addition to the fraud schemes described in the Indictment, Tsastsin and certain of his coconspirators also sold fake antivirus software to victims whose computers had been infected with scareware.

Other than the Rove Companies, Tsastsin also owned a domain registration company called EstDomains. EstDomains was notorious among network security/antivirus companies for registering websites for other cyber criminals engaged in various illegal schemes.[1]

---

[1] *See* http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html; http://www.informationweek.com/services/data/icann-shutting-down-estdomains-nov-24/212002478; http://www.secureworks.com/resources/blog/research/general-20841/.

Tsastsin also has a prior criminal history. He was convicted in Estonia in February 2008 of credit card fraud, money laundering, and document forgery.[2] As a result of Tsastsin's conviction, in late 2008, the Internet Corporation for Assigned Names and Numbers ("ICANN") – one of the main bodies responsible for governing the Internet and managing the routing of Internet addresses – revoked EstDomains' accreditation as a registrar, meaning that any IP address or domain name registered through EstDomains, for all practical purposes, would not exist on the Internet.

B. TIMUR GERASSIMENKO

Gerassimenko was the director of Infradata, which employed at least four Estonian code writers/programmers involved in the conspiracy, including co-defendant Dmitri Jegorov. Among the Estonian defendants, he was Tsastsin's closest associate, serving as Tsastsin's second-in-command and his confidant in all aspects of the fraudulent scheme. The following communications show the extent of Gerassimenko's knowledge of, and participation in, the Rove Digital criminal enterprise:

- Gerassimenko was involved in preventing antivirus programs from detecting the conspirators' malware. For example, in July 2008, Aleksejev sent Gerassimenko and Tsastsin an email attaching a screenshot from the Firefox/Mozilla search engine, which appeared to be part of an abuse complaint. The screenshot showed that the website "pcprivacycleaner.com" [i.e., a website the defendants operated or used to distribute their malware) had been blocked as an "attack site," which Firefox/Mozilla described as a site that tries "to install programs that steal private information, use your computer to attack others, or damage your system." In the email, Aleksejev explained that the default settings of the new Firefox search engine blocked websites with potentially unreliable programs. In response, Gerassimenko wrote, "It is necessary to find out the location where he [i.e., the individual who sent the screenshot] requests IE [i.e., Internet Explorer] phishing filter and Firefox, and block those f[]cking sites."

- Gerassimenko not only dealt with the programmers for the fraudulent scheme, but also the network administrators. For example, in July 2008, Ivanov, a network administrator, forwarded to Gerassimenko an email from an individual using the nickname "gfeed man." The email contained instructions on how to steal search data from Google without being blocked by Google's fraud detection algorithms. Gerassimenko, in turn, forwarded the instructions to Jegorov (the nominal employer of the conspiracy's Estonian network administrators) and told him to prepare a server and install on it the necessary script for stealing Google data. Jegorov complied, then emailed Gerassimenko the IP address of the new server and test results for the script.

[2] *See* http://www.icann.org/correspondence/burnette-to-tsastsin-28oct08-en.pdf.

- As another example of Gerassimenko's involvement in network administration, in August 2008, Aleksejev sent an email to Tsastsin that contained a hyperlink to an article on the website of a well-known antivirus company, entitled "Rogue Domain Name System Servers Part 2," attached hereto as Exhibit A. The article described "a network of more than 600 (apparently) identical rogue DNS servers, which IP addresses are hardcoded in DNS-changing malware" and the "remarkable advanced technical and social engineering tricks" that define the corresponding DNS-changing Trojans. The article provided examples of how certain domain names were resolved by the rogue DNS servers to different domains controlled by the conspirators and the IP addresses of those domains. The email was forwarded to Gerassimenko, who then told Jegorov to make changes to one of the IP addresses mentioned in the article.

- Gerassimenko participated in setting up contracts with ad brokers and selling hijacked clicks. For example, in a September 2008 email about setting up Gathi.com, a shell company that Tsastsin used to enter into contracts to sell hijacked clicks to ad brokers, co-defendant Taame asked Tsastsin, "Will Timur Gerassimenko sign contracts from your side?" As an alternative, Taame said, "If you want fake name, then signature should be fake as well. But if you pay taxes and not afraid of tying your name to spyware (what if Timur decides to go to [the] States), then everything could be signed honestly." Tsastsin responded "timur gerassimenko will be signee. He'll be a General Manager." Records from U.S.-based ad brokers showed that Gerassimenko was listed as the contact for Gathi.com on one advertising account, although a Copenhagen, Denmark address was given for Gathi.com. Phony information was similarly used to set up Gathi.com accounts with other ad brokers; none reflected any information that would alert the ad brokers to the fact that Gathi.com had links to Estonia, Russia, Rove Digital, or any of the conspirators. In September 2009, Gerassimenko asked Tsastsin why Gathi.com was set up instead of "some abstract domain name?" Tsastsin replied, "well, we had to use something[.] I think this domain is precisely that: abstract[.] nobody knows that gathi is ours."

- Gerassimenko also participated in stealing data from Google. For example, in November 2009, Gerassimenko asked Tsastsin whether he should send hijacked clicks from Google.uk and Google.ca to Taame's advertising accounts or their own. Tsastsin said to use their own account. Gerassimenko replied, "ok, then I'm setting up a new account on gathi and utter [i.e., UtterSearch, another shell company used to sell hijacked clicks]." Tsastsin then tested their online connection for stealing Google search results and found that "nothing is getting picked up." Gerassimenko explained that he had tested the connection earlier and it worked fine. He surmised that Rove Digital personnel "probably tested everything from the office [i.e., using Rove Digital's office Internet connection] and the office got banned" by Google's fraud detection algorithms and advised Tsastsin to close his sessions, then retry.

- In addition, Gerassimenko considered other ways to generate fraudulent Web traffic. For example, in June 2009, Gerassimenko forwarded to Aleksejev an email from Tsastsin. The

email read, in part: "Look the Indians don't want to give us the feeds but say let us put together whatever you need over here. Can we somehow send a person over to have him do the autoclicks over there? Or will the domain get seriously burned [i.e., identified as being used for illicit activity] and hit with abuse complaints?" Gerassimenko asked Aleksejev to "do some research whether it's possible to create an autoclick here through JS [javascript...."

- Finally, as Gerassimenko wrote in his letter to the Court, he developed websites for Rove Digital. Those websites included dummy websites which "laundered" hijacked clicks so that they appeared to come from the dummy websites rather than the websites that actually generated the clicks. They also included other websites which surreptitiously downloaded the DNS Changer Malware onto victims' computers.

C. Dmitri Jegorov

As discussed above, Jegorov was the nominal director of Novatech, which employed the network administrators involved in the conspiracy, including Ivanov. Jegorov was himself a programmer. Jegorov was responsible for managing the Rove Companies' sophisticated and far-flung network infrastructure. He also worked with Aleksejev to prevent DNS Changer-infected computers from obtaining antivirus software updates. According to Jegorov, he was paid USD 5,000 to 6,000 a month for working with Tsastsin. He, along with some others, also received unspecified sums in bonuses from Tsastsin.

D. Valeri Aleksejev

Aleksejev was initially hired as a programmer for Rove Digital in 2007. At the time of his arrest in November 2011, he was senior programmer for Infradata and reported directly to Gerassimenko. His responsibilities included devising ways to block DNS Changer Malware-infected computers from accessing antivirus software or operating system security updates, so that such software would not detect and remove the Malware; testing the Malware against various antivirus or operating system security programs to determine if they were capable of detecting the Malware hidden inside other software; and other programming projects to which he was assigned, including, for example, writing a program to conduct autoclicks on various websites in order to generate advertising revenue for the conspiracy. Aleksejev was sentenced to a term of 48 months' imprisonment.

E. Konstantin Poltev

Given the conspirators' reliance on online infrastructure, financial institutions and advertising networks around the globe to perpetrate their fraudulent scheme, Poltev's ability to communicate with them in nearly fluent English was indispensable to the success of their joint venture. Poltev joined Rove Digital in or about 2005 as a systems administrator. According to Poltev, he was not a good system administrator and therefore transferred to EstDomains. At

EstDomains, Poltev worked as the abuse manager, responding to numerous complaints about various domains and IP addresses registered to EstDomains that were used in various cybercrimes. After EstDomains' demise following ICANN's revocation of its registrar accreditation, Poltev transferred to IT Consulting. Because of Poltev's English-language ability, he was the public face of the conspiracy in its dealings with numerous foreign entities. For example, among other things, Poltev was responsible for handling abuse complaints about domains and IP addresses controlled by the Rove Companies, identifying advertising partners for Furox APS and responding to their complaints when they detected low-quality or fraudulent Internet traffic, and registering domains that were used in the fraud scheme.

F. Anton Ivanov

Ivanov joined Rove Digital in approximately late 2006 or early 2007 as a system administrator. His job was to set up and secure servers and install applications. While the other Estonian defendants appeared to have personal relationships that pre-dated their involvement in the conspiracy, the Government believes that Ivanov was only an employee. Poltev remarked in his post-arrest interview that Ivanov was a "small person" in the organization.

II. Sentencing Factors

For the reasons discussed below, the sentencing factors enumerated in 18 U.S.C. § 3553(a) strongly weigh in favor of a Guidelines sentence in this case.

A. Seriousness of the Offense

The offense was serious and extremely sophisticated. As discussed in the Indictment and the Presentence Report, Jegorov knowingly participated in a scheme to infect millions of computers worldwide with malware that blocked the computers' ability to update their antivirus protections and that turned the computers into instrumentalities of online advertising fraud for the coconspirators' own enrichment. At the time of their arrests, the defendants operated a vast network of servers, including approximately 50 rogue DNS servers located in New York City and additional servers at a data center in Chicago. Each of the rogue DNS servers contained approximately two hard drives. The servers with the larger hard drives received as many as 3,000 DNS resolution requests per second, while the smaller servers received several hundred requests per second.

The defendants' fraudulent scheme affected victims at numerous levels. At the most basic level, the victims included owners of infected computers who were prevented from visiting websites that they wanted to visit and from obtaining antivirus software updates. These victims include individuals, corporations, nonprofit organizations, and governmental entities. Given the large number of infected computers and victims, it is exceedingly difficult to estimate the total loss to this class of victims. However, as an example, the National Aeronautics and Space Administration, which had identified 135 incidents of DNS Changer infection in its network,

incurred approximately $65,755 in remediation costs. *See* Exhibit B, at 2. Dell SecureWorks, a network security company, estimated that its enterprise customers likely spent in excess of $4 million (including the costs of replacing infected computers and security staff time) to respond to the Malware. *See* Exhibit C, at 2. A university located in the mid-west identified 46 incidents of DNS Changer infection, primarily on personally owned computers that logged onto the university's network.[3] These figures represent the damage to only a small fraction of the total number of estimated victims.

Victims also included advertisers who lost Web visitors who were potential customers; website operators who lost advertising revenue as a result of Web traffic that should have gone to their sites being redirected elsewhere; and advertisers and website operators who paid for worthless Internet traffic in that the visitors landed on their website not due to any real interest, but because of click hijacking.

Another class of victims consisted of the search engines that suffered reputational harm. When Internet users clicked on search results and found themselves redirected to random sites, they blamed the search engine. As Google. explained:

> First and foremost, when infected users clicked on a link in their Google search results, they would sometimes be redirected to a website selected by the malware instead of the actual website displayed in the search results. In addition, some users would sign in to Google services, but then would immediately be signed out again due to the fact that users were being redirected through the defendants' proxies. . . .
>
> The impacted users were unaware that they were infected with malware and, from their perspective, Google was the cause of the issues they were experiencing.

See Exhibit D, at 1-2. As a result, some Google users switched to its competitors' search engines. According to Google, hundreds of thousands of users of its search engine had been compromised by the DNS Changer Malware. *See id.* at 2. Google was not alone. Using a DNS Changer-infected undercover computer, an agent found that when he conducted searches using some of the most popular search engines and clicked on links in the search results pages, many his clicks were hijacked to websites he had not intended to visit. Using the same infected computer, the agent also received error messages when he attempted to visit known websites for obtaining antivirus software updates.

[3] The university decided not to submit a letter to the Court, but provided the information to the Government.

Yet another class of victims were the antivirus companies that expended substantial resources to research complaints from their customers and fix the reported problems. For example, Dell SecureWorks estimated that it expended approximately $34,280 in responding to DNS Changer infections on its enterprise customers' computers.

Finally, the Government spent approximately $100,000 in remediation expenses. At the time the defendants were arrested, the FBI seized and disabled the defendants' rogue DNS servers. In order to ensure that infected computers that were connecting to the rogue DNS servers for DNS resolution did not suddenly lose the ability to access the Internet, the Government obtained judicial authorization to hire the not-for-profit organization Internet Services Consortium to replace the rogue DNS servers with legitimate DNS servers for a period of months, to give owners of infected computers time to fix their DNS settings and attempt to remove the Malware. The aggregate cost of that remediation effort amounted to approximately $100,000.

B. Need for Specific and General Deterrence and Just Punishment

Although the need for specific deterrence may be relatively low in this case, there is tremendous need for general deterrence. The anonymity of the Internet, the difficulty of determining which "clicks" are fraudulent, the huge sums of money involved in online advertising, the ability to spread the network infrastructure used to perpetuate click fraud across multiple countries, and the ease of operating far from where most victims are located, all combine to make online advertising fraud tempting to cyber criminals as a low-risk, high-reward proposition. A substantial sentence is therefore necessary to alter that perception in order to deter others from engaging in this type of cybercrime.

C. Characteristics of the Defendant

Gerassimenko has collaborated with Tsastsin since at least 2008. In his letter to the Court, Gerassimenko wrote that his business, Infradata was a website development company that had a lot of clients, presumably unrelated to the charged scheme. Assuming that were true, Gerassimenko had a legitimate source of income, yet chose to engage in crime. And, like his co-defendants in this case, Gerassimenko was undeterred by Tsastsin's prior conviction for credit card fraud and money laundering and resulting term of imprisonment, but instead continued to work with Tsastsin to expand their criminal enterprise. As the communications described above showed, Gerassimenko participated in virtually every aspect of the fraudulent scheme. His position of trust within the organization was demonstrated by the fact that he was designated as the director of one of the two key Rove Companies that were not mere shell companies, but actually employed staff to do the technical work necessary for the click hijacking scheme's success. A substantial amount of money – over $1.8 million – was sent through an account in the name of that company, which further demonstrated Tsastsin's trust in Gerassimenko.

D. The Probation Office's Recommended Sentence

The Government respectfully disagrees with the Probation Office's recommended sentence of 42 months' imprisonment. The recommended sentence would in fact create an unwarranted disparity with respect to Aleksejev, because as the discussion above makes clear, Gerassimenko was more highly placed within the organization than Aleksejev. The Government recognizes that the Stipulated Guidelines Range in Gerassimenko's plea agreement with the Government is lower than in Aleksejev's. However, that is in large part because the Government took into consideration the fact that Aleksejev received a sentence well below his Stipulated Guidelines Range. The Government therefore believed that while incorporating Aleksejev's higher Guidelines range into the agreement with Gerassimenko may have symbolic value, it would have little practical import. Accordingly, the Government did not seek the higher range. In short, Gerassimenko has already benefited from being sentenced later than Aleksejev. A further reduction is wholly unwarranted.

III. The Defendant's Estonian Sentence and Incarceration

Gerassimenko has been convicted in Estonia of money laundering and sentenced to one year and eight days of imprisonment. He was not charged with the underlying fraud and computer intrusion crimes in Estonia, in part because most of the victims of the crimes were in the United States and to avoid double jeopardy under Estonian law. To the Government's knowledge, he has been incarcerated continuously since his arrest on November 8, 2011, for a total of approximately three years and nine and a half months. The defense letter notes that Gerassimenko has to serve another 22 months of his Estonian sentence upon his return. However, it is the Government's understanding that he was only sentenced to one year and eight days of imprisonment in the Estonian case. We are attempting to clarify this with the Estonian authorities. In any event, according to the U.S. Bureau of Prisons, he will receive credit (one day for one day) toward his U.S. sentence for any time served that is not credited to his Estonian sentence.

Gerassimenko argues that the Court should impose a non-Guidelines sentence because of the poor conditions at Tallinn Prison, where he was incarcerated for approximately two years and seven and a half months (November 8, 2011, to June 27, 2015). While the Government has no first-hand knowledge of the conditions at the Tallinn Prison, it appears that the photos submitted by the defendant are from an Estonian-language newspaper article dated December 15, 2013. For the sake of completeness, the Government respectfully refers the Court to all of the photos from that article, which show both renovated and unrenovated parts of the same facility. *See* article available at: http://www.delfi.ee/news/paevauudised/eesti/delfi-fotod-reportaaz-kohast-kuhu-keegi-meist-sattuda-ei-taha?id=67442928. The Government has not been able to confirm in which section the defendant was housed.

It is the Government's understanding that the defendant intends to apply to the International Prisoner Transfer Program ("IPTP") to complete any sentence of imprisonment that

the Court may impose. In this connection, it should be noted that according to IPTP officials, under Estonia's parole policy, defendants are generally eligible for parole after serving 50 percent of their sentence, as opposed to 85 percent in the United States. Thus, any sentence that the Court imposes would, for all practical purposes, be reduced by half should the IPTP grants a transfer request. This fact is relevant in determining a sentence that adequately reflects the seriousness of the crime and affords adequate deterrence.

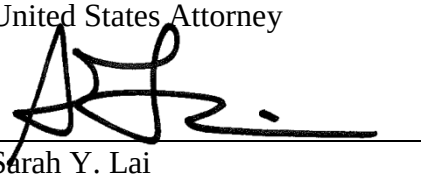
Finally, the Government respectfully requests, after conferring with the Bureau of Prisons ("BOP"), that the Court state on the record whether, in imposing sentence, the Court has, or has not, already reduced the term of imprisonment to account for the sentence in Estonia. For example, if the Court determines that a sentence at the bottom of the Guidelines range would be appropriate for the defendant's offense conduct, and deducts from that sentence the defendant's Estonian sentence of one year and eight days (even though it was for a different crime), it would assist the BOP to have that noted on the record.

CONCLUSION

For the reasons discussed above, the Government respectfully submits that a sentence within the Guidelines range of 78 to 97 months should be imposed, and that the previously submitted Consent Order of Forfeiture should be issued.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 
Sarah Y. Lai
Assistant United States Attorney
(212) 637-1944

cc: Glenn Garber, Esq.
(By electronic mail)